图书情报工作
第 65 卷 第 7 期　2021 年 4 月

电信诈骗情境下受害人欺诈信息接受意愿及其分享行为研究*

■ 李辉
中国人民公安大学公安管理学院　北京 100038

摘　要：[目的/意义] 基于个体信息行为发生动力理论，深入研究受害人诈骗信息接受意愿及其诈骗信息分享行为过程中不同影响因素间的作用机理，对于做好电信诈骗犯罪预防具有重要意义。[方法/过程] 基于"动机－机会－能力"(motivation-opportunity-ability，MOA)模型逻辑框架，从受害人动机因素、机会因素、能力因素三方面建构影响受害人欺诈信息接受意愿及其对欺诈信息分享行为的理论模型，借助 IBM-SPSS23.0 和 AMOS23.0 统计软件，通过问卷调查方法、多元统计回归方法对 1 398 个受害人调查样本进行实证分析和数据处理。[结果/结论] 性别和婚姻状况对于受害人接受欺诈信息意愿存在显著影响；虚假信息"权威性"、对欺诈人员的信任度以及自身贪利心理等动机因素是受害人产生欺诈信息接受意愿的重要驱动力；受害人自我效能感和网络安全识别能力对其欺诈信息接受意愿分别具有正向和负向显著影响，且两者均对欺诈信息接受意愿与其欺诈信息分享行为之间关系具有显著正向调节作用；受害人智能手机依赖程度、个体时间成本均对欺诈信息接受意愿与其欺诈信息分享行为之间的作用关系具有显著正向调节作用。结果表明，打击电信诈骗要多措并举，加强针对虚假信息、名人代言与各类媒体的监管，增强受害人网络安全识别能力，防范智能手机网络金融非理性投资。

关键词：电信诈骗　欺诈信息　受害人　接受意愿　分享行为
分类号：G252.7
DOI：10.13266/j.issn.0252－3116.2021.07.009

1　引言

随着电信网络的飞速发展，智能手机的普及度越来越高，网络借贷、金融互助、虚拟货币等电信诈骗犯罪已经超越传统刑事犯罪的发案数，成为我国新型犯罪的高发区和"重灾区"[1]。由于电信诈骗犯罪的隐蔽性强、跨区域广、技术侦查难度大等特点，致使该类案件案发后打击和追赃难度较大，被害人常因财产损失严重而导致"家破人亡"，从而严重影响社会安全稳定。该类案件，如"E 租宝"等涉众型电信诈骗犯罪，由于涉案人数多且涉案损失大，极易引发受害人群体性上访事件，如果处置过程不当，则可能会直接挑战和影响政府执政公信力[2]。鉴于电信诈骗近些年表现出的显著特点，如何科学有效预防电信诈骗已经成为制止此类案件发生的关键所在。相关研究的重心也从事后关注案件的侦破转向了事前犯罪预防，并开始逐渐重视受害人被骗诱因以及受害人被骗行为变化等方面的研究。

目前研究主要集中在 3 个方面：①考察客观特征与受害人被诈行为关系。从受害人性别来看，研究结论并不统一。如有研究认为男性受害者多于女性[3]，相反地，还有研究认为女性遭受电信诈骗犯罪的概率比男性高[4]，也有研究认为男性与女生被害概率相当，不存在显著差异[5]。从受害人所在地域看，地理区域因素与电信诈骗的被骗金额、被骗方式、资金转移通道均无显著相关，且受害人的流动性和分散性特征明显[6]。从受害人年龄特征看，受害人的被骗金额通常与被骗人的年龄成正比，而对于年龄特征在被害人群体的占比中，观点存在分歧。有学者根据被害人笔录的量化统计分析，指出 19－40 岁的年龄层在被害人中所占比重大[3]，因为该年龄段群体社会资源占有多，也易于接触网络贷款与投资理财诈骗[7]。但是其他学者则持不同观点，如有研究根据公安部 2009 年的抽样调查，分析得出中老年人被骗的比重较高[8]。②考察受害人心理特征与其被诈行为关系。关于电信诈骗被害人的心理特征因素分析，大致可归为两种路径。一种

* 本文系国家社会科学基金一般项目"涉众型经济犯罪受害人非理性信任行为与治理策略研究"(项目编号：20BGL253)研究成果之一。
作者简介：李辉(ORCID：0000－0001－9493－7934)，副教授，博士，博士生导师，E-mail：lihui0532@163.com。
收稿日期：2020－11－12　修回日期：2021－01－11　本文起止页码：90－102　本文责任编辑：易飞

路径为"弱势-信任"模式,如认为电信诈骗案件中被害人的弱势心理是犯罪人获得被害人信任的重要原因,并据此心理向被害人传输虚假信息,达到被害人"自愿"转账付款的目的[9]。该分析模式的优点是解释了犯罪人取得被害人信任的原因,但是对被害人本身的心理特征没有进行全面展开分析。另外一种路径为"趋利-避害"模式,这种研究路径认为电信诈骗被害人的心理特征可以分为趋利心理和避害心理,并且针对相关心理进行预防对策的探究。如有研究指出,被害人存在趋利和避害心理需求,并且犯罪人在取得信任之后利用上述心理需求对被害人进行操纵,进而获得其财物[10]。③考察受害人所处环境特征与其被诈行为关系。从社区环境特征因素来看,治安环境不好的社区居民、非全职工作者容易成为电信诈骗的被害人,居住在治安环境不佳的社区居民在电信诈骗人眼里更"好骗",并且非全职工作者居家的时间更长,接到诈骗电话的概率也更大[8]。

从已有研究看,目前研究在两个方面仍值得进一步深入探讨:①相关研究结论争议较大,尚未形成系统理论解释框架。已有研究关注到了人口统计学因素、心理因素和环境特征因素的影响,但尚未基于受害人被诈的深层诱因形成系统性理论解释框架,特别是鲜有研究从"受害人为何会接受欺诈信息"这一反映本质问题的视角解释电信诈骗生成原因。②定量化的实证研究偏少。目前研究多是以定性分析为主,而利用多元统计回归等实证研究方法进行诱因性质的因果定量分析则相对偏少,特别是缺少基于大样本数据刻画电信诈骗受害人接受欺诈信息本质规律方面的研究。基于此,本研究通过大样本数据分析,重点关注电信诈骗中受害人接受欺诈信息的意愿分析以及为何会将这些信息与他人分享的内在作用机理,致力于破解当前电信诈骗预防中的两大难题:①受害人为什么会接受欺诈信息?究竟哪些因素在驱动该意愿产生?②当受害人接受欺诈信息后,他们在什么情况下会将这些信息分享给周围他人?"传染"其他潜在受害人?受害人欺诈信息分享行为又是受制于哪些因素的影响?

为深度解决上述问题,本研究从受害人视角出发,借助"动机-机会-能力"(motivation-opportunity-ability,MOA)模型的逻辑框架,从"是否想做?"(动机因素)、"是否允许做?"(机会因素)以及"是否能做"(能力因素)等3个层面共同解释影响受害人接受诈骗信息的心理机制及其影响因素背后的理论逻辑和作用机理,并借助1 398个有效样本对理论假设进行实证分析,旨在为从受害人视角预防典型诈骗提供精准对策。

2 理论模型与研究假设

2.1 MOA模型与电信诈骗受害人欺诈信息分享行为

MOA模型最早由D. J. MacInnis和B. J. Jaworski[11]提出,主要是用来解释个体信息行为发生动力的综合性理论框架,该理论模型认为动机(motivation)、机会(opportunity)和能力(ability)三方面因素共同决定了个体的信息接受和处理行为。一般而言,MOA模型中的动机被认为是行动的直接驱动力(即"是否想做"),机会主要是影响动机与行为活动的限制性环境因素(即"是否允许做"),而能力则主要是指驱动行为产生所需要具备的技能水平(即"是否能做"),三者共同交互产生作用进而诱发个体行为发生[11-12]。因此,MOA模型的解释逻辑可以理解为:动机直接对行为产生影响,而机会和能力则是对动机-行为路径产生调节效应[13],见图1。从已有研究看,MOA模型在消费者广告信息处理[14]、民众公共关系管理[15]、民众社区参与行为[16]、组织社会资本[17]、知识共享[12]以及健康谣言传播[18]等领域被广泛应用且具有较强解释力。因此,本研究认为,该理论模型对于解释电信诈骗受害人信息接受意愿、信息分享行为同样具有解释力。因为在电信诈骗背景下,受害人分享欺诈信息的行为可以被视为是基于对欺诈信息虚假"权威性"、犯罪嫌疑人信任以及贪利心理等信息分享动机直接驱动下的一种信息接受行为(意愿)反映。同时,利用该模型还能解释电信诈骗受害人由欺诈信息接受动机到欺诈信息分享过程中的不同因素,如物理环境(智能手机媒介或其他)、时间环境(时间成本)、受害人网络安全预防能力以及自我效能感等多种因素对"动机-行为"路径产生影响的机制。此外,该模型对综合刻画电信诈骗受害人的信息接受动机及信息分享行为规律具有重要作用。下文将利用理论研究假设进行具体分析。

2.2 是否想做?——电信诈骗受害人欺诈信息接受意愿动机分析

动机一般是指意愿、兴趣和处理信息的愿望表达[14],是驱动个体产生内心愿望或意向的内在诱因[13],当个体的内在诱因被激活时,动机才会转化为行为。在电信诈骗背景下,当受害人不清楚所接触信息是欺诈信息时,他们容易被诈骗信息的虚假包装、犯罪分子的巧舌如簧以及内心的贪念所"俘获",成为电信诈骗的对象。首先,从欺诈信息层面看,犯罪分子往往会利用权威部门、权威媒体或权威人士来包装和释

放虚假信息[19]，利用虚假信息内容“勾住”目标进行欺骗，激发他们产生内在动机，进而促使他们产生接受欺诈信息的意愿。由此，本研究提出如下假设：

H1a：虚假信息的“权威性”越强，受害人的欺诈信息接受意愿越强烈。

其次，从犯罪分子层面看，大量电信诈骗犯罪分子会通过“小恩小惠”频繁地与受害人进行互动，在取得受害人人际信任的基础上实施最终欺骗的目的。按照信任转移理论，当受害人一旦对电信诈骗犯罪分子产生人际信任时，这种人际信任可能会随之转移至对犯罪分子所兜售的虚假产品信息的产品或服务信任。当然，在人际信任的动机驱动下，受害人也可能会更加乐于与周围他人分享该类信息。由此，本研究提出如下假设：

H1b：对犯罪分子的信任度越高，受害人的欺诈信息接受意愿越强烈。

再次，从受害人心理特征层面看，凡是被犯罪分子欺骗的受害人多数都是因为心有贪念，由贪图“蝇头小利”慢慢步入积重难返的被骗深渊。也可以说，贪利心理是诱发受害人接受欺诈信息的重要心理动机，也是他们产生欺诈信息分享行为的重要前置性动因[20]。由此，本研究提出如下假设：

H1c：受害人的贪利心理越强，其欺诈信息接受意愿越强烈。

2.3 是否允许做？——机会因素对电信诈骗受害人欺诈信息分享行为的影响分析

MOA 模型中的机会主要是指在特定时空里，以时间性和有利性为主要特征，对个体行为起推动或抑制作用的不受行为主体控制的外部环境要素[21]，是个体由动机转向行为时所面临的情境因素[18]，也是个体行动被“是否允许做”的外在影响因素。更进一步地，机会可以被视为是行为主体为达到某种预期，利用时间、注意力、可获得的重复次数等帮助或阻碍行为效果的因素[22]，既可以是创造有利情境的积极因素[14]，也可以是约束行动执行的消极因素。按照上述逻辑，在电信诈骗背景下，本研究认为有两个方面的因素会影响到受害人由欺诈信息接受意愿向欺诈信息分享行为的转变。一方面，就客观物理环境层面而言，本研究认为智能手机的使用依赖程度是影响欺诈信息快速传递的有利工具[23]，也可能是目前越来越多年轻受害人受骗的关键（因为仍有部分老年人不使用智能机）。在某种程度上讲，以智能手机作为信息传递工具不仅能够达到快速将欺诈信息分享出去的目标，同时也大大增加了受害人在不明情况下分享欺诈信息的速度。由此，本研究提出如下假设：

H2a：受害人智能手机使用的依赖程度越高，欺诈信息接受意愿对其信息分享行为的影响程度越大。

另一方面，本研究认为受害人面临的时间成本是影响其是否进行欺诈信息分享的另一重要决定性因素。知识分享领域的大量研究成果已经关注到，互联网背景下，时间成本成为限制个体处理和分享信息的重要因素[24-25]。在互联网时代，人们会面临较以往更多、更频繁的信息输入。对大量输入信息进行筛选并将其分享需要耗费一定的时间成本。因此，高机会是促使人们将电信诈骗信息（不明情况下的欺诈信息）作为“有价值信息”分享给身边重要他人的重要影响因素。相反，如果接受欺诈信息的时间成本较高，则可能会成为受害人对欺诈信息进行彼此分享的一种资源消耗，会在一定程度上抑制欺诈信息分享。由此，本研究提出如下假设：

H2b：时间成本越高，受害人欺诈信息接受意愿对其信息分享行为的影响程度越低。

2.4 是否能做？——电信诈骗受害人能力因素对其欺诈信息分享行为的影响分析

MOA 模型中的能力重点强调个体在一定社会关系中所具备的能够影响所从事活动完成度的内在可能性[13]。在电信诈骗背景下，现有研究已经证实受害人的经验和专业知识是他们抵抗电信诈骗伤害的重要方式。如具有较高网络体验和安全知识的人不太容易受到“网络钓鱼”诈骗企图的影响[26]。本研究认为，具备网络安全识别能力的人不仅会相对较少产生接受欺诈信息的动机，而且，这种专业能力还是有效阻断欺诈信息传递和分享的重要因素。因此，本研究提出如下假设：

H3a：受害人具备的网络安全识别能力越高，其欺诈信息接受意愿越低。

此外，受害人的自我效能感也可能是影响其欺诈信息分享的一个重要内在驱动因素。所谓自我效能感，主要是指个人对自己能够成功完成某种任务或胜任某种工作的自我能力评价。一般而言，当个体自我效能感较强时，他们自我感觉能够把控事态发展的预期和意愿也就越强烈。在电信诈骗背景下，某些受害人在接触欺诈信息之初尽管感觉可能不会“天上掉馅饼”，但他们往往可能会对自己的能力产生过度自信，最终陷入诈骗陷阱。换言之，电信诈骗一般是犯罪分子精心编织，甚至多次试验后的高级骗局，对消除受害

人戒心,逐步引其入局均作了缜密设计。所以,如果受害人过度自信,一旦入局,可能会难以脱身,甚至个别受害人在"禁果效应"的驱使下,明知可能是骗局还依然会选择好奇性尝试。因此,本研究提出如下假设:

H4a:受害人自我效能感越强,其欺诈信息接受意愿越高。

更进一步地,本研究认为,当受害人自我效能感较高,或他们具备了一定的网络安全识别技能时,他们会对自己的专业知识、专业技能更加自信。在电信诈骗背景下,受害人的这种自信可能更多属于过度自信,甚至某些网络安全识别技能也仅是对预防信息接受意愿层面起到作用,对其信息接受意愿到分享行为之间反而可能会起到反向助推作用,也可能会因此驱使其"自认为"拥有较高掌控力和较高专业网络安全技能的情况下,进而增加其欺诈信息接受意愿对其欺诈信息分享行为产生影响的程度。按照俗语来说,就是"河里淹死的更多的是会水的"。由此,可以合理推断,当受害人自我效能感较高或网络安全识别能力较高时,其可能会对"动机－行为"路径(欺诈信息接受意愿－欺诈信息分享行为)产生更强的调节作用。因此,本研究提出如下假设:

H3b:受害人具备的网络安全识别能力越高,欺诈信息接受意愿对其信息分享行为的影响程度越大。

H4b:受害人自我效能感越强,欺诈信息接受意愿对其信息分享行为的影响程度越大。

综上,本研究基于 MOA 模型建构如图 1 所示的理论解释模型。具体而言,按照 MOA 模型逻辑,欺诈信息分享行为的产生会受到动机、机会和能力的共同影响。结合上述理论假设,在电信诈骗情境下,本研究认为欺诈信息接受意愿是影响受害人欺诈信息分享行为的重要动机之一,是最为直接的影响因素(即为模型中的"M",直接决定"是否想做")[13]。并且,如图 1 最左侧所示,本研究从欺诈信息、欺诈人员以及受害人 3 个方面将可能促使受害人产生欺诈信息接受意愿(即产生"动机")的因素分别归纳为虚假信息"权威"、信任度以及贪利心理等 3 种驱动因素。同理,MOA 模型中的"机会"因素主要是影响和制约行为能否产生的外部工具或限制性环境因素,对个体行为产生具有间接调节效应。在本研究中,我们将受害人对智能手机的依赖程度和他们面临的决策时间成本,作为影响其产生欺诈信息分享行为过程中的重要制约因素(即为模型中的"O",决定外在条件"是否允许做")。更进一步地,按照 MOA 模型逻辑,本研究将受害人的自我效能感和网络安全识别能力作为影响其产生(或避免)欺诈信息行为所具备的关键"能力",而受害人的这些关键技能亦会对其行为产生间接的调节作用(即为模型中的"A",决定"是否能做")。综合而言,本研究认为,在电信诈骗情境下,受害人的"动机"因素(欺诈信息分享意愿)、"动机"驱动因素(虚假信息"权威"、信任度以及贪利心理)、"机会"因素(智能手机依赖程度和时间成本)以及"能力"因素(自我效能感和网络安全识别能力)共同影响其欺诈信息分享行为的产生,其中,"动机"因素是最直接的影响因素,而"机会"和"能力"因素则是通过间接调节效应影响受害人欺诈信息分享行为。

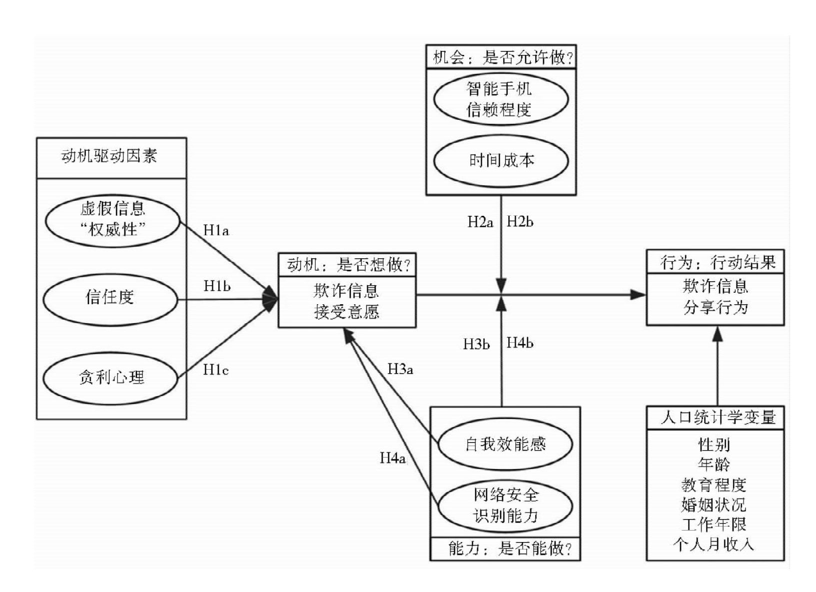


图 1　本研究理论模型

3 研究设计与验证性因子分析

3.1 研究设计

3.1.1 样本来源及样本结构

本研究样本主要采用便利抽样方法对曾经遭遇过电信诈骗的受害人进行问卷调查,调查时间为2019年4月至2019年12月,共发放问卷1 500份,收回问卷1 427份,剔除无效问卷后保留1 398个有效样本。在调查问卷中本研究设置"您是否遭遇过电信诈骗案(事)件? 若没有该类经历,请您终止本问卷填写"这一测项来识别目标群体。同时,利用"您遭受电信诈骗过程中,是否在并不知情的时候将欺诈信息分享(或转发、口头传递等)至其他人?"这一问题,对没有欺诈信息传播行为的被试也进行了剔除。此外,本研究样本结构从各个人口统计学变量的数量和占比上看,具有一定的代表性,如表1所示:

表1 本研究样本结构(N=1 398)

样本特征	分类标准	样本		样本特征	分类标准	样本	
		数量/人	百分比/%			数量/人	百分比/%
年龄	18-25岁	414	29.6	教育程度	小学及以下	364	26.0
	26-30岁	184	13.2		初中	70	5.0
	31-40岁	424	30.3		高中和中专	652	46.6
	41-50岁	282	20.2		大学专科	184	13.2
	51-60岁	71	5.1		大学本科	115	8.2
	61-65岁	7	0.5		研究生	13	0.9
	65岁以上	16	1.1	工作年限	1年及以下	399	28.5
性别	女性	574	41.1		2年	85	6.1
	男性	824	58.9		3-5年	121	8.7
个人月收入	3 000元及以下	462	33.0		6-10年	212	15.2
	3 001- 6 000元	539	38.6		11-20年	349	25.0
	6 001-10 000元	191	13.7		20年以上	232	16.6
	10 001-20 000元	166	11.9	婚姻状况	已婚	818	58.5
	20 001-50 000元	25	1.8		未婚	549	39.3
	50 000元以上	15	1.1		离婚	24	1.7

3.1.2 变量测量

本研究主要采用7级李克特量表方法对相关变量进行赋值和测量(见表2)。虚假信息"权威性"主要是指受害人被骗前所接触到的诈骗分子对欺诈信息进行的"权威性"虚假包装,该量表主要参考X. Luo等[19]和P. Fischer等[20]的文献研究思路设计,共3个测项,其Cronbach's α信度系数为0.890;信任度量表主要是指受害人对涉案人员的人际互动信任,其量表主要参考R. C. Mayer等[27]和J. Gould-Williams[28]等的文献研究思路设计,共包括3个测项,其Cronbach's α信度系数为0.869;贪利心理主要是指受害人在被骗前贪图电信诈骗利益的心理状态,该量表主要参考葛悦炜[8]和马李芬等[29]的文献研究思路设计,共包含3个测项,其Cronbach's α信度系数为0.911;智能手机依赖程度量表主要是指被害人使用智能手机的频率,该量表主要借鉴A. Vishwanath[23]的文献研究思路设计,主要包括3个测项,其Cronbach's α信度系数为0.905;时间成本主要是指受害者关注欺诈信息所愿意花费的时间和精力,主要参考宋小康等[18]和J. Wang等[30]的文献研究思路设计,主要包括3个测项,其Cronbach's α信度系数为0.868;自我效能感主要是指受害人对自己能够成功完成相关网络投资理财的自我能力评价,主要参考明均仁等[31]学者的研究成果设计,主要包括3个测项,其Cronbach's α信度系数为0.942;网络安全识别能力主要是指受害人具有一定的网络安全意识并能够识别一定的网络安全风险,该量表主要参考B. Harrison等[32]的研究思路设计,主要包括3个测项,其Cronbach's α信度系数为0.895;欺诈信息接受意愿主要是指受害人积极主动接受欺诈信息的意愿,该量表主要借鉴贾明霞等[12]的知识交流与共享意愿的思路进行设计,主要包括3个测项,其Cronbach's α信度系数为0.858;欺诈信息分享行为主要是指受害人在不明真相的情况下积极主动分享欺诈信息的行为,该量表主要借鉴贾明霞等[12]的知识交流与共享行为的思路进行设计,主要包括3个测项,其Cronbach's α信度系数为0.833。此外,本研究邀请了8位相关领域专家对所有改编变量及其测量内容的准确性进行多轮论证,确保所有变量具有较高内容效度。

表 2　本研究各变量测量及信度系数(N = 1 398)

变量名称	维度	测项或赋值	因子载荷	Cronbach's α 系数
动机驱动因素	虚假信息“权威性”	受骗前,我了解的信息有“官方”通知、认证	0.80	0.890
		受骗前,我了解的信息有名人代言或背书	0.91	
		受骗前,我了解的信息有知名媒体报道	0.85	
	信任度	受骗前,我对诈骗人员的工作能力非常信任	0.81	0.869
		受骗前,诈骗人员对我非常关心	0.88	
		受骗前,我认为诈骗人员很有诚意	0.80	
	贪利心理	受骗前,我收到了很多“小恩小惠”的利益	0.86	0.911
		受骗前,我承认我是有些贪婪的心理	0.88	
		受骗前,我认为该项投资(或产品)有利可图	0.89	
机会因素	智能手机依赖程度	我每天使用智能手机的时间平均在 6 小时以上	0.84	0.905
		我很难想象没有智能手机的时刻	0.89	
		我经常使用智能手机处理各项事情	0.90	
	时间成本	我会在利用网络搜寻和关注投资理财相关信息上花费大量时间	0.85	0.868
		我愿意为了解投资理财相关信息投入时间	0.87	
		我会花费大量时间主动研究网上投资理财信息	0.78	
能力因素	自我效能感	被骗前,我觉得我很有自信能够单独完成网络投资理财任务	0.87	0.942
		被骗前,我有信心能够单独解决网络投资理财过程中遇到的难题	0.94	
		被骗前,我觉得我能够完成好之前没有接触过的网络投资理财任务	0.95	
	网络安全识别能力	被骗前,我感觉自己具有很强的网络安全意识	0.92	0.895
		被骗前,我认为自己能够识别一些网络骗人小伎俩	0.77	
		被骗前,我认为自己能够防范一定的网络安全风险	0.89	
欺诈信息接受意愿	—	被骗前,我会积极地浏览网络投资理财信息并接受相关信息	0.81	0.858
		被骗前,我会尽量让其他人也能够接受和分享我的网络投资理财信息	0.78	
		被骗前,我会极力向亲朋好友推荐网络投资理财信息或产品	0.77	
欺诈信息分享行为	—	被骗前,我经常通过网络与其他人分享我购买投资理财产品的经验	0.85	0.833
		被骗前,我经常主动推送给亲朋好友有关网络投资理财的信息	0.85	
		被骗前,我经常将我的网络投资理财信息或产品推荐给自己最信任的人	0.79	

3.1.3　共同方法偏差检验

共同方法偏差检验主要为了应对数据来源相同、样本采集环境、采集语境等因素诱发的预测变量与效标变量之间人为的共变,这种变化可能会给研究结论带来一定偏差,因此,需要对问卷测量中可能出现的这种现象进行检验,一般学界多采用周浩和龙立荣推荐的单因素检验方法进行检验[33]。从表 3 中的单因子模型检验结果可知,其拟合结果并不理想(如 RMSRA = 0.143 > 0.08),由此,可以从侧面说明本研究样本并不存在严重的共同方法偏差,可以进行下一步的实证分析。

3.2　验证性因子分析

限于篇幅,本研究对问卷量表设计前的电信诈骗受害人深度访谈资料以及调查问卷的预测试探索性因子分析结果的校正等前期工作不再赘述(问卷形成前,共对 36 名电信诈骗受害人进行了深度访谈)。所以,本研究直接展示利用 AMOS23.0 软件对不同因子模型进行分析验证后的结果。其中,单因子是将所有观察变量放在一起;二因子模型是将动机因素、机会因素、能力因素以及欺诈信息接受意愿因子所有观察变量聚合成一个因子,与欺诈信息分享行为因子组合而成;三因子模型是将动机因素、机会因素、能力因素的所有观察变量聚合成一个因子,欺诈信息接受意愿单独作为一个因子,与欺诈信息分享行为因子组合而成;四因子模型是将动机因素所有观察变量聚合成一个因子,机会因素、能力因素的所有观察变量聚合成一个因子,欺诈信息接受意愿单独作为一个因子,与欺诈信息分享行为因子组合而成;六因子模型是将机会因素、能力因素的所有观察变量聚合成一个因子,与虚假信息“权威性”、信任度、贪利心理、欺诈信息接受意愿、欺诈信息分享行为等因子组合而成;八因子(a)模型是将机会因素的所有观察变量聚合成一个因子,与虚假信息“权威性”、信任度、贪利心理、自我效能感、网络安全识别能力、欺诈信息接受意愿、欺诈信息分享行为等因子组合

而成；八因子(b)模型是将能力因素的所有观察变量聚合成一个因子，与虚假信息“权威性”、信任度、贪利心理、智能手机依赖程度、时间成本、欺诈信息接受意愿、欺诈信息分享行为等因子组合而成；九因子模型是将虚假信息“权威性”、信任度、贪利心理、智能手机依赖程度、时间成本、自我效能感、网络安全识别能力、欺诈信息接受意愿、欺诈信息分享行为等因子组合而成，是本研究的主要模型。

验证性因子分析结果(见表 3)显示九因子模型的各项指标明显优于其他模型，这在一定程度上说明本研究设定基本模型具有良好区分效度，也说明本研究设定的理论模型具有一定的可行性。此外，表 2、本研究各变量相关关系表(见表 4)显示本研究各因子载荷均在 0.5 以上，且 AVE 的值均大于 0.5，均满足学界对收敛效度的要求。

表 3 本研究验证性因子分析结果(N = 1 398)

模型	χ^2	df	χ^2/df	RMSEA	GFI	CFI	NFI
九因子模型	1 228.1	288	4.26	0.076	0.90	0.98	0.97
八因子模型(a)	3 982.8	296	13.46	0.094	0.80	0.90	0.89
八因子模型(b)	2 899.0	296	9.79	0.079	0.85	0.93	0.92
六因子模型	4 784.7	309	15.48	0.102	0.87	0.88	0.87
四因子模型	6 859.2	318	21.57	0.121	0.67	0.83	0.82
三因子模型	7 648.6	321	23.83	0.128	0.64	0.80	0.80
二因子模型	8 803.1	323	27.25	0.137	0.64	0.77	0.77
单因子模型	9 539.5	324	29.44	0.143	0.57	0.75	0.75

3.3 各变量相关关系

本研究中虚假信息“权威性”、信任度、贪利心理、智能手机依赖程度、时间成本、自我效能感、网络安全识别能力、欺诈信息接受意愿、欺诈信息分享行为等变量之间呈现明显相关关系(见表 4)，说明可以进行下一步的实证分析。

表 4 本研究各变量相关关系(N = 1 398)

变量	均值	方差	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
年龄	3.56	1.68	—															
性别	0.59	0.24	0.098	—														
未婚	0.39	0.24	-0.80	-0.076	—													
离婚	0.02	0.017	0.092	-0.013	-0.106	—												
教育程度	4.78	1.27	-0.15 **	-0.068 *	0.131 **	-0.003	—											
工作年限	3.52	3.58	0.856 *	0.096 **	-0.799	0.107 **	-0.124	—										
个人月收入	2.14	1.26	0.406	0.136	-0.421	0.033	0.261 *	0.471 *	—									
虚假信息“权威性”	4.94	2.35	0.019	0.034	-0.039	0.038	-0.008	0.024	-0.004	0.73								
信任度	4.79	1.85	-0.006	0.017	-0.008	0.029	-0.011	-0.009	-0.040	0.57 ***	0.69							
贪利心理	4.89	1.81	-0.012	0.004	-0.015	0.046	-0.007	-0.032	-0.059 *	0.62 ***	0.68 ***	0.77						
智能手机使用依赖程度	4.55	2.26	-0.009	0.037	-0.017	0.019	-0.009	-0.021	-0.040	0.59 **	0.58 ***	0.68 ***	0.77					
时间成本	5.10	1.99	-0.006	0.071 **	-0.014	0.033	-0.016	-0.007	-0.022	0.38 ***	0.64 ***	0.47 ***	0.61 ***	0.70				
自我效能感	4.47	2.70	0.012	0.045	-0.037	0.016	-0.025	-0.009	-0.025	0.221 **	0.641 **	0.330 **	0.33 ***	0.47 ***	0.85			
网络安全识别能力	4.551	2.30	-0.015	0.032	-0.009	0.004	-0.008	-0.027	-0.045	0.30 ***	0.16 ***	0.51 **	0.39 ***	0.69 ***	0.59 ***	0.74		
欺诈信息接受意愿	5.07	1.64	-0.026	0.056 *	0.000	0.054 *	0.023	-0.027	-0.033	0.49 **	0.62 **	0.56 **	0.56 ***	0.59 ***	0.53 ***	-0.58 **	0.62	
欺诈信息分享行为	3.56	1.68	-0.005	0.065 *	-0.019	0.063 *	0.014	-0.008	-0.018	0.544 **	0.592 **	0.57 ***	0.60 ***	0.59 **	0.59 **	-0.62 **	0.81 ***	0.70

注：* $p < 0.05$，** $p < 0.01$，*** $p < 0.001$，对角线为变量 AVE 的值

4 实证检验

本研究主要利用 IBM-SPSS23.0 软件采用逐步回归的方法对人口统计学控制变量、虚假信息“权威性”、信任度、贪利心理、自我效能感、网络安全识别能力对欺诈信息接受意愿的直接效应进行实证检验。此外，采用多元回归方法对智能手机依赖程度、时间成本、自我效能感、网络安全识别能力的调节效应进行实

证检验,具体如下:

4.1 直接效应检验

直接效应回归结果(见表5)显示,采用逐步回归方法依次将人口统计学控制变量、虚假信息"权威性"、信任度、贪利心理、自我效能感、网络安全识别能力等变量依次放入模型1至模型6的回归方程中,可得:

模型1的结果表明,与女性相比,男性有更加强烈的欺诈信息接受意愿(β=0.046,P<0.05);与其他婚姻状况相比,离婚状态下的民众对欺诈信息的接受意愿更强(β=0.047,P<0.05)。模型2的结果显示,在模型1的基础上将虚假信息"权威性"变量放入回归方程后,虚假信息"权威性"对民众欺诈信息接受意愿具有显著正向影响(β=0.521,P<0.001),假设H1a得到验证。模型3的结果显示,在模型2的基础上,将信任度变量放入回归模型后,信任度对民众欺诈信息接受意愿具有显著正向影响(β=0.552,P<0.001),假设H1b得到验证。模型4的结果显示,在模型3的基础上将贪利心理变量放入回归模型后,贪利心理对民众欺诈信息接受意愿具有显著正向影响(β=0.316,P<0.001),假设H1c得到验证。模型5的结果显示,在模型4的基础上将自我效能感放入回归模型后,自我效能感对民众欺诈信息接受意愿具有显著正向(β=0.309,P<0.001),假设H4a得到验证。模型6的结果显示,在模型5的基础上将网络安全识别能力放入回归模型后,网络安全识别能力对民众欺诈信息接受意愿具有显著负向影响(β=-0.109,P<0.001),假设H3a得到验证。

此外,从回归结果来看,方差膨胀系数VIF值均在10以内,说明并不存在严重多重共线性;DW值为2.046,非常接近2,说明该回归方程也不存在明显的序列相关问题。由此,上述研究结论具有一定的科学性。

表5 直接效应回归结果(N=1 398)

变量	欺诈信息接受意愿					
	模型1	模型2	模型3	模型4	模型5	模型6
年龄	0.015	0.032	0.029	0.020	0.016	0.023
性别	0.046*	0.027	0.025	0.028	0.024	0.023
未婚	-0.044	-0.008	0.000	0.021	0.028	0.026
离婚	0.047*	0.030	0.024	0.018	0.021	0.026
教育程度	0.031	0.028	0.026	0.023	0.025	0.020
工作年限	-0.034	-0.037	-0.025	0.006	0.016	0.012
个人月收入	-0.053	-0.037	-0.016	-0.005	-0.008	-0.001
虚假信息"权威性"		0.521***	0.206***	0.095***	0.070***	0.058***
信任度			0.552***	0.402***	0.341***	0.265***
贪利心理				0.316***	0.265***	0.241***
自我效能感					0.309***	0.381***
网络安全识别能力						-0.109***
R^2	0.007	0.276	0.481	0.526	0.559	0.561
ΔR^2	0.007	0.270	0.205	0.045	0.033	0.002
F值	1.30	66.30***	143.03***	154.11***	159.60***	147.51***
DW值	2.046					

注:$^{*}p<0.05$,$^{**}p<0.01$,$^{***}p<0.001$

4.2 机会因素的调节效应检验

由于本研究涉及变量较多,故采用G. Ahuja[34]推荐的逐步回归方法对相关变量的调节效应进行检验。为在一定程度上防止调节效应交互项中多重共线性的出现,在进行调节效应检验之前,本研究将对相关变量进行中心化处理,中心化处理后的变量前加"Z"以示区分(因性别、婚姻状况等为类别变量,未做中心化处理,但为了与前文有所区别,下文中的类别变量前面也加了"Z")。机会因素中的智能手机依赖程度和时间成本的调节效应检验效果如表6所示。由模型7、模型8以及模型9的结果可知,在智能手机依赖程度(β=0.595,p<0.001)和欺诈信息接受意愿(β=0.683,p<0.001)均对欺诈信息分享行为具有显著影响的基础上,增加欺诈信息接受意愿与智能手机依赖程度的交互项,模型9的解释力有所提升(ΔR^2=0.003,p<0.001),且交互项显著(β=0.058,p<0.01),因此,智能手机依赖程度对其欺诈信息接受意愿与欺诈信息分享行为之间关系具有显著的正向调节效应,即受害人

智能手机使用的依赖程度越高,其欺诈信息接受意愿对其信息分享行为的影响程度越大,假设 H2a 得以检验。同理,由模型 10、模型 11 以及模型 12 的结果可知,在时间成本($\beta = 0.582$, $p < 0.001$)和欺诈信息接受意愿($\beta = 0.667$, $p < 0.001$)均对欺诈信息分享行为具有显著影响的基础上,增加欺诈信息接受意愿与时间成本的交互项,模型 12 的解释力虽有所提升($\Delta R^2 = 0.003$, $p < 0.001$),且交互项显著($\beta = 0.054$, $p < 0.01$),但是,交互项符号与预期假设相反,因此,时间成本对其欺诈信息接受意愿与欺诈信息分享行为之间关系具有显著的正向调节效应,即受害人花费的时间成本越高,其欺诈信息接受意愿对其信息分享行为的影响程度反而越大,与前文理论假设不一致,假设 H2b 没有通过检验。此外,从各回归方程的 VIF 值和 DW 值来看,均在临界值以内,说明本研究结论具有一定的可信性。

表 6 机会因素的调节效应回归结果(N = 1 398)

变量	欺诈信息分享行为					
	模型 7	模型 8	模型 9	模型 10	模型 11	模型 12
Z 年龄	−0.016	−0.031	−0.032	−0.003	−0.027	−0.026
Z 性别	0.047 **	0.037 **	0.036 **	0.029	0.030	0.029
Z 未婚	−0.020	−0.039	−0.035	−0.043	−0.041	−0.037
Z 离婚	0.052 **	0.028	0.029	0.044 *	0.026	0.026
Z 教育程度	0.025	0.009	0.007	0.032	0.011	0.010
Z 工作年限	−0.001	−0.011	−0.011	−0.029	−0.017	−0.017
Z 个人月收入	−0.011	0.001	0.003	−0.022	−0.001	0.000
Z 智能手机依赖程度	0.595 ***	0.133 ***	0.121 ***	—	—	—
Z 时间成本	—	—	—	0.582 ***	0.174 ***	0.184 ***
Z 欺诈信息接受意愿		0.683 ***	0.698 ***		0.667 ***	0.667 ***
Z 欺诈信息接受意愿 * 智能手机依赖程度			0.058 **			
Z 欺诈信息接受意愿 * 时间成本						0.054 **
R^2	0.364	0.615	0.619	0.348	0.625	0.628
ΔR^2	0.364	0.252	0.003	0.348	0.277	0.003
F 值	99.32 ***	246.82 ***	225.08 ***	92.72 ***	256.75 ***	233.70 ***
DW 值	—	—	1.979	—	—	1.954

注: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

4.3 能力因素的调节效应检验

与上文调节效应处理方法相同,本部分能力因素调节效应同样采用逐步回归方法,实证结果见表 7。由模型 13、模型 14 以及模型 15 的结果可知,在自我效能感($\beta = 0.614$, $p < 0.001$)和欺诈信息接受意愿($\beta = 0.668$, $p < 0.001$)均对欺诈信息分享行为具有显著影响的基础上,增加欺诈信息接受意愿与自我效能感的交互项,模型 15 的解释力有所提升($\Delta R^2 = 0.002$, $p < 0.001$),且交互项显著($\beta = 0.050$, $p < 0.01$),因此,受害人自我效能感对其欺诈信息接受意愿与欺诈信息分享行为之间关系具有显著的正向调节效应,即受害人自我效能感越高,其欺诈信息接受意愿对其信息分享行为的影响程度越大,假设 H4b 得以检验。同理,由模型 16、模型 17 以及模型 18 的结果可知,在网络安全识别能力($\beta = 0.590$, $p < 0.001$)和欺诈信息接受意愿($\beta = 0.670$, $p < 0.001$)均对欺诈信息分享行为具有显著影响的基础上,增加欺诈信息接受意愿与网络安全识别能力的交互项,模型 18 的解释力有所提升($\Delta R^2 = 0.006$, $p < 0.001$),且交互项显著($\beta = 0.076$, $p < 0.001$),因此,网络安全识别能力对其欺诈信息接受意愿与欺诈信息分享行为之间关系具有显著的正向调节效应,即受害人所具备的网络安全识别能力越高,其欺诈信息接受意愿对其信息分享行为的影响程度越大,假设 H3b 得以检验。此外,从各回归方程的 VIF 值和 DW 值来看,亦均在临界值以内。

5 结论与讨论

5.1 研究结论

随着信息化的普及和金融市场的开放,普通民众的金融投资渠道越来越多,但也面临着较大的被诈骗风险。本文依托 MOA 理论逻辑框架,从受害人动机因素、机会因素和能力因素 3 个方面建构了影响受害人欺诈信息接受意愿及其对欺诈信息分享行为的理论模型,并利用 1 398 个受害人调查样本实证检验了本文

李辉.电信诈骗情境下受害人欺诈信息接受意愿及其分享行为研究[J].图书情报工作,2021,65(7):90－102.

表 7　能力因素的调节效应回归结果(N = 1 398)

变量	欺诈信息分享行为					
	模型 13	模型 14	模型 15	模型 16	模型 17	模型 18
Z 年龄	-0.017	-0.031	-0.031	-0.033	-0.036	-0.034
Z 性别	0.049 **	0.037 **	0.036 **	0.045 *	0.035 *	0.036 *
Z 未婚	-0.023	-0.038	-0.035	-0.011	-0.034	-0.030
Z 离婚	0.060	0.031	0.032	0.054 *	0.029	0.029
Z 教育程度	0.024	0.009	0.008	0.036	0.012	0.010
Z 工作年限	0.001	-0.011	-0.010	0.020	-0.004	-0.005
Z 个人月收入	-0.007	0.001	0.002	-0.021	-0.001	0.002
Z 自我效能感	0.614 ***	0.153 ***	0.147 ***	—	—	—
Z 网络安全识别能力	—	—	—	0.590 ***	0.162 ***	0.155 ***
Z 欺诈信息接受意愿		0.668 ***	0.676 ***		0.670 ***	0.679 ***
Z 欺诈信息接受意愿 * 自我效能感			0.050 **			
Z 欺诈信息接受意愿 * 网络安全识别能力						0.076 ***
R^2	0.387	0.618	0.621	0.357	0.621	0.627
ΔR^2	0.387	0.231	0.002	0.357	0.265	0.006
F 值	109.52 ***	249.54 ***	226.78 ***	96.27 ***	253.20 ***	233.37 ***
DW 值	—	—	1.978	—	—	1.975

注:* $p<0.05$, ** $p<0.01$, *** $p<0.001$

的理论假设,共得到如下结论:

(1)受害人群体中男性比女性更可能接受欺诈信息,且处于离婚状态的受害人比其他婚姻状况的受害人更容易接受欺诈信息。不仅如此,本研究对欺诈信息分享行为的人口统计学变量进行回归分析时,也有同样发现,即男性比女性具有更强烈的欺诈信息分享行为,离婚状态的受害人较其他人更容易产生欺诈信息分享行为。本文推测男性比女性更容易接受和分享欺诈信息的原因可能在于:在中国中青年家庭中,与女性相比,男性更多地在承担供养家庭生活的主要角色,他们面临相对较大的工作和生活压力,他们会寻找更多途径去投资理财,因此,接受欺诈信息的可能性相对较高;而对于老年家庭而言,大量女性老年人在退休阶段承担起照顾子女孩子的责任,但男性老年人则可能更有闲暇和机会接触欺诈信息,也更容易被欺诈信息蒙骗。此外,本文推测,与其他婚姻状态相比,处于离婚状态的人群可能有更强的意愿去获得经济收入,且更多情况下他们对财产具有独立决策权(相对已婚状态和未婚状态,且未婚大部分经济收入不稳定),更容易受到欺诈信息的欺骗,亦更容易产生分享行为。

(2)虚假信息"权威性"、对欺诈人员的信任度以及自身贪利心理等动机因素对受害人接受欺诈信息的意愿具有直接且显著的影响,是受害人产生欺诈信息接受意愿的重要驱动力,是影响受害人"是否想做"(即接受欺诈信息)的本源因素之一。从现实案例中可知,大部分电信诈骗案例都有涉案人员通过虚假"官方"信息、权威人士或知名媒体包装自己的经历,这是诈骗信息取得受害人认同的第一步。通过虚假信息骗取受害人认同后,电信诈骗犯罪分子与受害人之间的网络互动,或给予受害人一些短期的"小恩小惠"以此借助其贪利心理来取得受害人信任,进而诱使受害人上当受骗是当前电信诈骗广为采用的手段。本研究实证结果也证实了虚假信息"权威性"、对欺诈人员的信任度以及自身贪利心理等动机因素对促使受害人产生接受欺诈信息的意愿均具有显著的影响,是启动受害人产生接受相关欺诈信息的关键因素。本研究结论与国外学者 P. Fischer 等[20]的研究发现具有一定的吻合性,即受害人对"官方"通知、标识等信息具有较高的接受意愿,该类虚假信息内容对于"勾住"受害目标进行欺骗很重要。更进一步地,本研究结论能够为源头阻断受害人"是否想"接受电信诈骗信息提供一些基本对策:①强化对涉网络金融投资产品或服务相关官方信息的监督核查力度,多渠道防控虚假信息对受害人产生负面影响;②通过增加网络金融产品相关人员信息公开力度,减少受害人因信息不对称而对诈骗犯罪分子产生非理性信任;③加强有关反诈信息的宣传力度,避免受害人因一时贪利心理受害、受骗,多途径增强防范"庞氏骗局"等电信诈骗手段。

(3)受害人自我效能感和网络安全识别能力对其欺诈信息接受意愿分别具有正向和负向显著影响,且

两者均对欺诈信息接受意愿与其欺诈信息分享行为之间具有显著正向调节作用。从本研究结论可知,从能力因素视角来看,对于受害人"是否能"接受欺诈信息还取决于两方面的自身因素:①本研究证实,若受害人被骗前具有较高自我效能感,他们陷入电信诈骗陷阱的可能性更高。②本研究实证结果显示,具有较高网络安全识别能力则对于预防电信诈骗具有显著抑制作用,如 R. T. Wright 和 K. Marett 在研究中发现,具备较高网络体验与安全知识的人不太容易受到网络诈骗的影响[26]。从上述两方面的结论来看,可以进一步推知:电信诈骗往往是犯罪分子精心设计,甚至是他们多次试验后的精密骗局,一般受害人受骗前很难通过自身金融专业方面能力将其完全识破,反而可能会因为受害人较高自我效能感导致"聪明反被聪明误"的后果,也可能会因受害人过度自信而自食恶果,因此,本研究结论对警示受害人投资网络金融产品风险具有一定启发。本研究结论还证实,若受害人拥有一定的网络安全识别能力则可能会减少被电信诈骗的可能,这也提示潜在受害人在投资网络金融产品时自主学习或是借助专门渠道掌握一些网络安全识别技能的必要性。换言之,本研究结论可以归纳为,在进行网络金融投资时,一方面切不可因自己拥有一定的金融专门知识或自认为掌握了网络金融投资技巧就盲目自信,这可能是导致投资者陷入诈骗陷阱的主要主观因素之一;另一方面,投资者也不必因电信诈骗难以预防就对网络投资"因噎废食",可以尝试通过增强网络安全识别能力来减缓被骗风险,如 B. Harrison 在研究中指出的个体自身的网络安全能力不能单独解释其如何成为网络诈骗的受害者[32]。然而,更进一步地,从受害人能力两个因素的调节效应来看,本研究发现,受害人一旦对欺诈信息具有接受意愿之后,无论是自我效能感还是网络安全识别能力都可能成为增加其分享欺诈行为的"助推器"。也就是说,当受害人进入电信诈骗信息骗局后,其个人能力因素越强,也就越是可能影响周围他人成为下一个电信诈骗的受害者,这是目前电信诈骗造成危害波及范围广、社会影响大以及"传染性"强的重要原因。

(4)从机会因素层面看,受害人智能手机依赖程度越高,其欺诈信息接受意愿对其欺诈信息分享行为产生的影响越大;受害人时间成本越高,其欺诈信息接受意愿对其欺诈信息分享行为的促进作用也越大。智能手机已经成为人们日常生活的重要组成部分,是我们进行消费、投资的重要手段,尤其是随着新冠肺炎的常态化防控,无接触式支付更是加速了智能手机的使用频率。本研究结论表明,智能手机使用的依赖程度可能是影响电信诈骗信息传播、加速受害人向潜在受害人传播的重要工具。在受害人接受欺诈信息后,他们的内在动机将会在智能手机工具的影响下,加速受害人欺诈信息分享行为的发生。此外,时间成本的调节效应虽然与前文理论假设产生了截然相反的结论,即时间成本越高,受害人分享欺诈信息的行为越强。该研究结论似乎有违一般常识,但仔细分析却有其合理性:虽一般而言,花费的时间成本越高,人们越不愿意参与,但因电信诈骗信息在被识破前往往具有较强的吸引力且会预期(或已经)给潜在受害人带来了一定的经济收益,这样便会大大增加受害人的时间投入,而这些时间投入也可能是他们向其他人进行分享和推荐的重要内在动力。

5.2 研究贡献与局限

本研究的主要贡献在于:①基于 MOA 模型的理论逻辑,从动机因素、能力因素和机会因素等多个层面建构了能够揭示电信诈骗背景下受害人接受欺诈信息意愿及其分享行为的本质规律,并经过实证检验验证了该理论模型的现实解释力,在理论层面具有一定的推动作用。②本研究结论能够为基于受害人能力、受害人心理、受害人使用媒介等多个层面预防电信诈骗信息以及阻断受害人欺诈信息"传染"周围潜在受害人提供有力的决策支撑,对打击电信诈骗顶层制度设计上,注重加强针对虚假信息、名人代言、各类媒体的监管,增强受害人网络安全识别能力以及防范智能手机网络金融非理性投资等相关政策措施具有重要现实贡献。除此之外,本研究也存在一些局限:①本研究属于事后研究电信诈骗受害人行为,可能与真实的电信诈骗受害人心理历程会有一定偏差,未来需要依靠实验研究方法更加真实的测度受害人行为规律;②本研究旨在勾勒受害人欺诈信息接受意愿和分享行为的基本影响因素的路径,但现实情况中的受害人信息接受意愿和分享行为可能还会受到诸如外部环境、产品体验忠诚等更多因素的影响而随之发生变化,因此,未来需要探索更多的研究变量来丰富和完善本研究理论框架;③本研究在问卷设计中更多地是将电信诈骗信息的类型聚焦在了"投资理财相关信息"方面,对健康类等其他诈骗信息的考虑不够全面。因此,未来研究需要聚焦分析更多的电信诈骗类型来进一步检验本研究结论的稳健性和科学性。

参考文献:

[1] 靳高风,守佳丽,林晞楠. 中国犯罪形势分析与预测(2018－2019)[J]. 中国人民公安大学学报(社会科学版),2019,35(3):1－11.

[2] 张莹,程传杰. 涉众型非法集资犯罪的实证分析与防控建议[J]. 中国检察官,2019(9):40－42.

[3] 殷明. 电信诈骗案件受害人的实证研究——基于受害人笔录的量化统计分析[J]. 中国刑警学院学报,2017(3):57－62.

[4] 苑景惠. 基于"二八定律"的电信诈骗犯罪防范机制研究[J]. 长春师范大学学报,2019, 38(5):34－37.

[5] 高蕴嶙,周玉玲. 大数据背景下电信诈骗犯罪侦防对策实证研究——以C市公安机关立案情况为分析样本[A]//中国犯罪学学会预防犯罪专业委员会,上海政法学院刑事司法学院－警务学院. 犯罪学论坛(第五卷). 上海:中国法制出版社,2018:880－887.

[6] 马忠红. 论网络犯罪案件中的抽样取证——以电信诈骗犯罪为切入点[J]. 中国人民公安大学学报(社会科学版),2018,34(6):69－78.

[7] 纪熙全. 电信网络诈骗犯罪的打击与防范——以福建省三明市为例[J]. 中国刑事警察, 2019(6):6－10.

[8] 葛悦炜. 电信网络诈骗防范宣传策略研究——基于电信网络诈骗被害人角度[J]. 公安学刊(浙江警察学院学报),2018(4):78－84.

[9] 蔡国芹,赵增田. 论电信诈骗犯罪立体防控体系的构建[J]. 犯罪研究,2011(4):99－105.

[10] 宋平. 电信网络诈骗的心理解析及其防控[J]. 广西警察学院学报,2017,30(1):121－ 125.

[11] MACINNIS D J, JAWORSKI B J. Information processing from advertisements: toward an integrative framework[J]. Journal of marketing, 1989, 53(4): 1－23.

[12] 贾明霞,熊回香. 虚拟学术社区知识交流与知识共享探究——基于整合S-O-R模型与MOA理论[J]. 图书馆学研究,2020(2):43－54.

[13] 陈则谦. MOA模型的形成、发展与核心构念[J]. 图书馆学研究,2013(13):53－57.

[14] MACLNNIS D J, MOORMAN C, JAWORSKI B J. Enhancing and measuring consumers' motivation, opportunity, and ability to process brand information from ads [J]. Journal of marketing, 1991, 55(4): 32－53.

[15] HALLAHAN K. Enhancing motivation, ability, and opportunity to process public relations messages [J]. Public relations review, 2000, 26(4): 463－480.

[16] HUNG K, SIRAKAYA-TURK E, INGRAM L J. Testing the efficacy of an integrative model for community participation[J]. Journal of travel research, 2011, 50(3): 276－288.

[17] ADLER P S, KWON S-W. Social capital: prospects for a new concept[J]. Academy of management review, 2002, 27(1): 17－40.

[18] 宋小康,赵宇翔,宋士杰,等. 基于MOA理论的健康谣言分享意愿影响因素研究[J]. 情报学报,2020,39(5):511－520.

[19] LUO X, ZHANG W, BURD S, et al. Investigating phishing victimization with the heuristic-systematic model: a theoretical framework and an exploration[J]. Computers & security, 2013, 38(5): 28－38.

[20] FISCHER P, LEA S E G, EVANS K M. Why do individuals respond to fraudulent scam communications and lose money? the psychological determinants of scam compliance[J]. Journal of applied social psychology, 2013, 43(10): 2060－2072.

[21] BARANOWSKI T, SMITH M, BARANOWSKI J, et al. Low validity of a seven-item fruit and vegetable food frequency questionnaire among third-grade students[J]. Journal of the American Dietetic Association, 1997, 97(1): 66－68.

[22] MCALEXANDER J H, SCHOUTEN J W, KOENIG H F. Building brand community[J]. Journal of marketing, 2002, 66(1): 38－54.

[23] VISHWANATH A. Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks[J]. Computers in human behavior, 2016, 63(5): 198－207.

[24] REINHOLT M, PEDERSEN T, FOSS N J. Why a central network position isn't enough: the role of motivation and ability for knowledge sharing in employee networks[J]. Academy of management journal, 2011, 54(6): 1277－1297.

[25] BRENNAN L L. Understanding the knowledge-sharing challenge: is a "bottleneck" perspective the answer? [J]. Academy of management perspectives, 2008, 22(3): 112－114.

[26] WRIGHT R T, MARETT K. The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived[J]. Journal of management information systems, 2010, 27(1): 273－303.

[27] MAYER R C, DAVIS J H. The effect of the performance appraisal system on trust for management: a field quasi-experiment [J]. Journal of applied psychology, 1999, 84(1): 123－136.

[28] GOULD-WILLIAMS J. The importance of hr practices and workplace trust in achieving superior performance: a study of public-sector organizations [J]. The international journal of human resource management, 2003, 14(1): 28－54.

[29] 马李芬,吕尧. 高校电信诈骗犯罪的解析及治理路径[J]. 北京警察学院学报,2017(4):110－114.

[30] WANG J, HERATH T, CHEN R, et al. Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email[J]. IEEE transactions on professional communication, 2012, 55(4): 345－362.

[31] 明均仁,余世英,杨艳妮,等. 面向移动图书馆的技术接受模型构建[J]. 情报资料工作,2014, 35(5):49－55.

[32] HARRISON B, SVETIEVA E, VISHWANATH A. Individual processing of phishing emails: how attention and elaboration protect against phishing[J]. Online information review, 2016, 40(2): 265－281.

[33] 周浩,龙立荣.共同方法偏差的统计检验与控制方法[J].心理科学进展,2004(6):942-950.
[34] AHUJA G. Collaboration networks, structural holes and innovation: a longitudinal study[J]. Academy of management proceedings, 2000,45(3):425-455.

Research on the Willingness of the Victim to Receive Fraud Information and Its Sharing Behavior in the Context of Telecom Fraud

Li Hui
School of Pulice Administration, People's Public Security University of China, Beijing 100038

Abstract: **[Purpose/significance]** From the perspective of information transmission, it is of great significance to analyze the mechanism of the process of "Persuading" the victims by the fraud information and sharing the fraud information, which is of great significance for the prevention of telecom fraud. **[Method/process]** Based on the logic framework of motivation-opportunity-ability (MOA) model, a theoretical model was constructed from three aspects of the victim's motivation, opportunity and ability factors, which affected the victim's willingness to receive fraud information and their behavior of sharing fraud information. With the help of IBM-SPSS23.0 and AMOS23.0 statistical software, questionnaire survey and multivariate statistics were conducted regression analysis and data processing were carried out on 1398 victims survey samples. **[Result/conclusion]** Gender and marital status have significant influence on the victim's intention to receive fraud related information; the "authority" of false information, the trust of fraud related personnel and their own greedy psychology are the important driving forces of the victims' intention to receive fraud related information; the victim's self-efficacy and network security identification ability have a significant positive and negative impact on their intention to receive fraud related information, and both of them have a significant positive moderating effect on the receiving intention of fraud related information and the sharing behavior of fraud related information; the frequency of the victim's smartphone use and individual time cost have a significant positive moderating effect on the intention to receive fraud related information and the behavior of sharing fraud related information. The results show that to crack down on telecom fraud, we should take various measures simultaneously, strengthen the supervision of false information, celebrity endorsements and various media, enhance the network security identification ability of victims, and prevent the irrational investment of smart phone network finance.

Keywords: telecom fraud　fraud information　victim　receiving intention　sharing behavior